IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
v.	)	Case No. 1:19-MJ-393
DANIEL RICHARD WILSON, II,	)	**UNDER SEAL**
Defendant.	)	

AFFIDAVIT IN SUPPORT OF A
CRIMINAL COMPLAINT AND ARREST WARRANT

I, Jenny M. Cutalo-Patterson, a Special Agent with the Federal Bureau of Investigation ("FBI"), Washington Field Division, Washington, D.C., being duly sworn, depose and state as follows:

1. I have been employed with the FBI since October 2005, and am currently assigned to the Washington Field Office, Northern Virginia Resident Agency ("NVRA"). Since joining the FBI, I have investigated violations of federal law involving Counterintelligence matters and currently investigate federal violations concerning child pornography and the sexual exploitation of children. I have gained experience in conducting such investigations through formal classroom training and on-the-job training. I have been involved in investigations involving the exploitation of children, including offenses involving the dissemination of child pornography on the internet via computer.

2. I submit this affidavit in support of a criminal complaint and arrest warrant charging the defendant, DANIEL RICHARD WILSON, II ("WILSON"), with receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) & (b)(1). For the reasons set forth below, I

submit that probable cause exists to believe that in or about October 2018, WILSON knowingly received child pornography in Bristow, Virginia, which is within the Eastern District of Virginia.

3. The statements contained in this affidavit are based on my experience and background as a Special Agent working in the area of child exploitation and child pornography, on information provided by other law enforcement agents and other individuals, and on my review of reports and records. Because I submit this affidavit for the limited purpose of securing a criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts believed necessary to establish probable cause for the requested criminal complaint and arrest warrant.

APPLICABLE STATUTES

4. Section 2252(a)(2) of Title 18 of the United States Code prohibits the knowing distribution and receipt of any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer. For purposes of this affidavit, "visual depiction[s] of minors engaging in sexually explicit conduct," will be referred to as "child pornography."

5. The term "minor," as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.

6. The term "sexually explicit conduct," as defined in 18 U.S.C. § 2256(2)(A)(i)–(v), means actual or simulated: (a) sexual intercourse, including genital-genital, oral-genital, anal genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or

pubic area of any person.

7. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data that is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

SUMMARY OF PROBABLE CAUSE

8. This case involves the unlawful receipt of images and videos depicting child pornography via a specific internet-based peer-to-peer ("P2P") network (the "Network"). As described below, I submit that probable cause exists to believe that in or about October 2018, WILSON knowingly received child pornography at his residence in Bristow, Virginia, within the Eastern District of Virginia

I. Background on P2P File-Sharing Networks and the Network

9. Based on my training and experience, I know that P2P file sharing is a method of communication available to internet users through the use of special software programs or clients. P2P file-sharing programs allow groups of computer users using the same file-sharing network and protocols to transfer digital files from one computer system to another while connected to an online network.

10. In order to access the Network relevant to this case, a user must first download the Network's software, which is free and publicly available online. Anyone running the Network's software may join and access the Network. Each computer running the Network connects directly to other computers running the Network, which are called its "peers." When installing the Network, each user agrees to provide to the Network a portion of the storage space on the user's computer hard drive so that files uploaded by the Network's users can be distributed and

stored across the network. The Network's users can upload files onto the Network and download files from the Network. After a user installs the Network on the user's computer, the software creates a default "download" folder. If a user successfully downloads a particular file from the Network, the Network will save the content of that file to the "download" folder. A user may change this default setting and direct the content to be saved elsewhere.

11. When a user uploads a file into the Network, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored on computers throughout the network of peers. The software also creates an index piece that contains a list of all of the pieces of the file and a unique key—a series of letters, numbers, and special characters—that is used to download the file. In order to download a file on the Network, a user must have the key for the file.

12. When a user attempts to download a file via the Network using the file's key, the Network downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Network's software then requests all of the pieces of the file from the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on.

II. Search of WILSON's Residence

13. In or about July 2018, during the course of an investigation, law enforcement observed that an individual connected to the Network from a specific IP address appeared to be requesting to download multiple child pornography files using the Network. Law enforcement then determined that this IP address was assigned to a residence in Bristow, Virginia, during the relevant time period and obtained a federal warrant to search the property from the United States District Court for the Eastern District of Virginia.

14. On or about October 18, 2018, law enforcement agents executed the warrant on

the property. Prior to the execution of the warrant, law enforcement queried publicly available databases, which revealed that WILSON resided alone at the residence. The warrant permitted law enforcement to, among other things, search the residence for evidence relating to the receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2).

15. During the search, law enforcement observed that WILSON appeared to live there alone. Law enforcement seized several electronic devices from the home, including a customized computer tower ("computer") and a WD My Passport Ultra external hard drive ("external hard drive").

16. WILSON was present at the residence during the search and agreed to speak to law enforcement. During the interview, WILSON confirmed that he lived alone at the residence and that no one else had regular access to the computer. He acknowledged to law enforcement that he had used file-sharing software before, including the Network. WILSON said that he recalled seeing links advertising child pornography when using P2P software, but denied ever viewing or downloading child pornography. WILSON told law enforcement that the files he downloaded using the Network would save to a "downloads" folder within the Network's installation folder. He also told law enforcement, however, that he had uninstalled the Network from his computer and that the Network's "downloads" folder was automatically deleted as a result.

III. Forensic Examination of WILSON's Devices

17. After seizing the computer and the external hard drive, law enforcement personnel forensically examined the devices. The examination uncovered hundreds of image and video files that appear to depict child pornography, as well as forensic evidence that WILSON downloaded child pornography using the Network.

18. Specifically, on the computer, the user of the device conducted a keyword search

for the Network on or about October 12, 2018. Likewise, the executable file used to install the Network's software was downloaded to the external hard drive on or about October 12, 2018, and the Network had been installed.[1] Inside a "downloads" folder located in a folder associated with the Network on the external hard drive were at least seven videos, including:

a. An approximately 22 minute video entitled "N1.mp4" that was created on or about October 12, 2018. The video depicts, among other things, what appears to be two nude, minor girls who are communicating with someone on a computer while being filmed by the computer's webcam. As the video progresses, the two girls move to a bed where they appear to touch each other's genitals;

b. An approximately 27 minute video entitled "N2.mp4" that was created on or about October 12, 2018. The video depicts, among other things, what appears to be the same two minor girls from the video entitled "N1.mp4" communicating with someone on the computer and then engaging in oral sex; and

c. A video entitled "suckit.mpg" that was created on or about October 12, 2018, and depicts what appears to be a minor girl engaged in oral sex with an adult male.

19. The forensic examination recovered hundreds of additional files of suspected child pornography located outside the Network's "downloads" folder on the external hard drive. The majority of these files were recovered as "orphan" files on the external hard drive, meaning that the "parent" application that generated or was associated with these files had been removed or uninstalled from the device. These videos include:

---

[1] An executable file is a digital file that ends with the filename extension ".exe" and will perform a certain function, like running or installing a program, when opened on a computer device. The Network's installer executable file, for example, will initiate the steps necessary to install the Network once it is opened.

a. An approximately 35 minute video entitled "[redacted]baby3bate.avi" that was created on or about April 18, 2018.[2] The video depicts, among other things, what appears to be three minor girls communicating with someone using a computer while being filmed by the computer's webcam. As the video progresses, the girls undress and then expose and touch their vaginas.

b. An approximately nine and a half minute video entitled "Webcam 12yo boy & 10yo girl Handjob e pleasuress.avi" that was created on or about April 19, 2018. The video depicts what appears to be a prepubescent girl masturbating the erect penis of a minor boy while being filmed by a computer's webcam; and

c. A video entitled "pthc-suckdick-19.avi" that was created on or about April 19, 2018.[3] The video depicts what appears to be an approximately three- to four-year-old girl engaged in oral sex with an adult male.

20. Additionally, the user of the external hard drive accessed multiple video files with titles that match the titles of these orphaned files of child pornography. At the time the user accessed these video files, they were stored on the external hard drive in a "downloads" folder associated with the Network. For example, on or about April 18, 2018, the user of the external hard drive accessed a video saved in the Network's "downloads" folder with a title that matches the video identified above in Paragraph 18(a). Similarly, on or about April 19, 2018, the user of the external hard drive accessed a video saved in the Network's "downloads" folder with a title that matches the video identified above in Paragraph 18(b). In fact, between about April 16 and

[2] The full title of the video is known to law enforcement but is redacted here out of an abundance of caution because it contains what may be a reference to the name of a minor victim depicted in the video. *See* 18 U.S.C. § 3509.

[3] Based on my training and experience, I know that the term "pthc" stands for "preteen hardcore" and is a term commonly used by individuals with a sexual interest in children to describe images and videos depicting minors engaged in sexual conduct.

April 19, 2018, the user of the external hard drive viewed at least or about nine video files with titles indicative of child pornography that were saved in the "downloads" folder associated with the Network.

21. Finally, orphaned versions of the Network's executable file were also recovered from the external hard drive. These files had creation dates of June 13, 2016, and March 16, 2018.

CONCLUSION

22. Based on the foregoing, I respectfully submit that there is probable cause to believe that in or about October 2018, in the Eastern District of Virginia, DANIEL RICHARD WILSON, II, knowingly received child pornography, in violation of 18 U.S.C. § 2252(a)(2) & (b)(1), and I therefore request that a criminal complaint and arrest warrant be issued for WILSON.

Respectfully submitted,

Jenny M. Cutalo-Patterson

Jenny M. Cutalo-Patterson, Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me
this 9th day of September, 2019.

/s/
Michael S. Nachmanoff
United States Magistrate Judge
The Honorable Michael S. Nachmanoff
United States Magistrate Judge